AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

2002 Buick Century, Silver, Virginia Tag: RCA 25
VIN: 2G4WS52JO21246234

Case No. 3:17SW37

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment "A".

located in the Eastern District of Virginia, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment "B".

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1038(a)(1)	Threats and Hoaxes
18 U.S.C. § 844(i)	Destruction of Building by Fire or Explosives

The application is based on these facts:

See attached Affidavit, which is fully incorporated by reference herein.

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

FBI SA Robert Wright
Printed name and title

Sworn to before me and signed in my presence.

Date: 3/14/2017

/s/
Roderick C. Young
United States Magistrate Judge

City and state: Richmond, VA

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF:

2002 Buick Century, Silver
Virginia Tag: RCA 25
VIN: 2G4WS52JO21246234

Probable location:
7447 Strawhorn Drive
Mechanicsville, VA 23116

Case No. 3:17SW37

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Robert L. Wright, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the vehicle known 2002 Buick Century, Virginia Tag number RCA 25, VIN# 2G4WS52JO21246234, probable location of 7447 Strawhorn Drive, Mechanicsville, VA 23116, hereinafter "VEHICLE," further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been since June of 2016. I have received specialized training in evaluating and searching vehicles for evidence both at the FBI Academy, and as a member of the FBI Richmond Division Evidence Response Team. Standard procedure in Richmond Division will likely include a

member of the Computer Analysis Response Team (CART) on this search. CART team members are highly specialized in evaluating and seizing computers and digital evidence.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

4. Subject of Richmond Federal Bureau of Investigation (FBI), Madison Legrand Jones, visited the Richmond FBI Office on February 10, 2017, and was interviewed by SA Robert Wright and Task Force Officer (TFO) Heath Brannagan. Jones had voluntarily come to the FBI office to explain the comments he had made in an online "tip" to the FBI's Public Assistance Line on February 9, 2017. In the "tip," he had written that he was going to "legally shoot at the FBI, then blow it up". Jones showed Wright and Brannagan a picture that he had taken of the FBI building, that he had enlarged. Jones was reluctant to comment on his motivations. He abruptly ended the interview, and drove away in a silver Buick Century, tag number RCA 25.

5. Jones was detained on March 3, 2017, at approximately 7:00 PM, at the National Security Agency (NSA) facility, Fort Meade Maryland. Jones was driving a silver 2002 Buick Century, tag number RCA 25, VIN 2G4WS52JO21246234, when he was detained. Jones was forcibly removed from the vehicle, after being uncooperative. Jones was admitted to a Baltimore area hospital for mental evaluation.

6. During a cursory search of the vehicle, officers noted metal handcuffs, and some audio visual equipment.

7. While Jones was being detained by officers, a two-page, printed list of approximately fifteen local, state, and Federal facilities was also found in the vehicle, with a comment at the top of the first page reading "Places to shoot; then blow up." This list was taken by officers at the scene.

8. Earlier in the day, on March 3, 2017, Jones also attempted to gain entry to the main Department of Justice (DOJ) building in Washington D.C. He became confrontational with security when he was denied entry, and was observed by security crossing Constitution Avenue, and getting into a Buick Century, tag number RCA 25.

9. Jones attempted to gain vehicle access to a Central Intelligence Agency facility, in the Washington D.C. area, on March 2, 2017, at approximately 9:49 PM. Jones was turned away, and was not detained. The report states the he was driving a 2002 Buick Century, tag number RCA 25.

10. On March 8, 2017, Richmond FBI was notified by Special Agent Brook Donovan, a Task Force Officer (TFO) with the FBI's Baltimore Division, that he had received information that there were also SD type storage cards identified in the vehicle during Jones's detention at NSA. Official police report from NSA is pending. During this time, the vehicle was in storage at a private facility after being towed from NSA.

11. On March 9, 2017, FBI Baltimore notified Richmond that the Buick Century had been removed from the towed car lot by members of Jones's family, and that the vehicle was possibly on the way back to the Richmond area.

12. On March 10, 2017, at approximately 5:30 PM, SA Robert Wright observed the Buick Century in the driveway at 7447 Strawhorn Drive, Mechanicsville, VA 23116, where Madison Legrand Jones lives with his mother, Jacqueline Jones.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

13. As described above and in Attachment B, this application seeks permission to search for records that might be found in the VEHICLE, in whatever form they are found. One form in which the records might be found is data stored on audio visual equipment or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

14. *Probable cause.* I submit that if audio visual equipment or storage medium is found in the VEHICLE, there is probable cause to believe those records will be stored on that equipment or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little

or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Depending on a variety of factors, a particular computer could easily not overwrite deleted files with new data for many months, and in certain cases conceivably ever.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is

typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

15. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the VEHICLE because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file

systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether

data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to commit a crime, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

16. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

17. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

18. Because several people share the VEHICLE, it is possible that the VEHICLE will contain storage media that are predominantly used, and perhaps owned, by persons who are not

suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

19. It appears that Mr. Click Photography ("the Company") is a functioning company operated by Madison Legrand Jones (not listed with the Virginia State Corporation Commission) that appears to conduct legitimate business. The seizure of the Company's equipment and storage media may limit the Company's ability to conduct its legitimate business. As with any search warrant, I expect that this warrant will be executed reasonably. Reasonable execution will likely involve conducting an investigation on the scene of what equipment, or storage media, must be seized or copied, and what equipment or storage media need not be seized or copied. Where appropriate, officers will copy data, rather than physically seize equipment or storage media, to reduce the extent of disruption. If employees of the Company so request, the agents will, to the extent practicable, attempt to provide the employees with copies of data that may be necessary or important to the continuing function of the Company's legitimate business. If, after inspecting the equipment and storage media, it is determined that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the government will return it.

SPECIFICITY OF SEARCH WARRANT RETURN

20. Consistent with the Court's current policy, the search warrant return will list the model(s) and serial number(s) of any and all equipment or storage media seized in the SUBJECT VEHICLE, and include a general description of any and all associated peripheral equipment that

has been seized. Additionally, the search warrant return will include the total numbers of each type of digital media that has been seized (*e.g.*, "ten (10) 3.5" diskettes; twenty (20) CDs; twenty (20) DVDs; three (3) USB drives; one (1) 256 MB flash memory card," *etc.*)

NOTICE REGARDING INITIATION OF FORENSIC EXAMINATION

21. Moreover, the Government will file a written pleading in this case within one hundred twenty (120) days after the execution of the search warrant notifying the court that the imaging process of digital evidence seized from the target location is complete, and the forensic analysis of computers and media has begun. Such notice will include confirmation that written notice has been provided to the defendant or his counsel informing the defendant that the forensic examination of evidence seized from him has actually begun. Such notice to the defendant and the Court is not intended to mean, and should not be construed to mean, that the forensic analysis is complete, or that a written report detailing the results of the examination to date will be filed with the Court or provided to the defendant or his counsel. This notice does not create, and is not meant to create, additional discovery rights for the defendant. Rather, the sole purpose of this notice is to notify the defendant that, beyond the simple seizure of his property, a forensic search of that property has actually begun.

CONCLUSION

22. I submit that this affidavit supports probable cause for a warrant to search the VEHICLE described in Attachment A and seize the items described in Attachment B.

Respectfully submitted,

ROBERT L. WRIGHT
Special Agent
FEDERAL BUREAU OF INVESTIGATION

Subscribed and sworn to before me
on March 13, 2017:

/s/
Roderick C. Young
United States Magistrate Judge

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be searched

The property to be searched is a silver 2002 Buick Century sedan, Virginia tag number RCA 25, VIN 2G4WS52JO21246234. Vehicle is registered to Beatrice Goldberg, believed to be Madison Legrand Jones's grandmother.

ATTACHMENT B

Property to be seized

1. All records relating to violations of **18 U.S.C. § 1038(a)(1) and 18 U.S.C. § 844(i)**, those violations involving **Madison Legrand Jones** and occurring after **February 9, 2017**, including:

   a. **Specifically, any computer or storage device, and associated storage media, which is located in the 2002 Buick Century sedan, VIN 2G4WS52JO21246234, used by Madison Legrand Jones for the purposes of perpetuating false information and hoaxes, and for specifying or encouraging any attempts to damage or destroy by means of fire or explosives any building, vehicle, or other real or personal property used in interstate or foreign commerce, especially any computer or storage device used for maintaining Madison Legrand Jones's Facebook page.**

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

   a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. records of or information about Internet Protocol addresses used by the COMPUTER;

j. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

k. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.